UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/841,689 | 04/23/2001 | Stephen Sorkin | RECOP008 | 4377 |

21912 7590 02/22/2005

VAN PELT & YI LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

| EXAMINER | |
|---|---|
| BAUM, RONALD | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

DATE MAILED: 02/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No.<br>09/841,689 | Applicant(s)<br>SORKIN ET AL. | |
|---|---|---|---|
| | Examiner<br>Ronald Baum | Art Unit<br>2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *22 October 2004*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *3,4,9,29,30 and 35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3,4,9,29,30,35* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

## DETAILED ACTION

1. This action is in reply to applicant's correspondence of 22 October 2004.

2. Claims 3,4,9,29,30,35 are pending for examination.

3. Claims 3,4,9,29,30,35 remain rejected.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

The term "possible" in claims 3,4,9,29,30,35 relative term rejection is withdrawn.

The phrase "method further" in claims 38,39 rejection is withdrawn.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 3,4,9,29,30,35 remain rejected under 35 U.S.C. 102(e) as being anticipated by Crosbie et al, "IDIOT - Users Guide", Technical Report TR-96-050, Perdue University, September 4, 1996.

5. As per claim 3; "A method for analyzing a logfile produced by a computer network security system [entire document, as per description in Chapter 5] comprising:

providing a regular expression query associated with a pattern to be searched for in the logfile [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the (i.e., C++) pattern programs).]; and

using the query to search for the pattern in the logfile [entire document, as per description in Chapter 4 (i.e., audit trail)];

wherein the pattern is associated with a *sgid* exploit and

using the query to search for the pattern includes

searching for entries showing that a process has been started by a sgid process with

effective group ID equal to zero [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the pattern programs (i.e., pages 2,3,6,10-13,16,29-35,59) whereas the explicit and implicit use of sgid term is taught (pages 6,25,30,50-54,60), and further, the effective group ID equal to zero is the same as granted super-user or root permission status).] and

group ID (gid) not equal to zero.";

And further as per claim 29; this claim is the apparatus of the method claim 3, and is rejected for the same reasons provided for the claim 3 rejection above;

And further as per claim 35; this claim is the embodied software on computer readable media of the method claim 3, and is rejected for the same reasons provided for the claim 3 rejection above.

6. Claim 4 ***additionally recites*** the limitations that; "The method as recited in claim 3, wherein using the query to search for the pattern further includes

storing a process ID of the process, and

searching for processes with a parent process ID equal to the stored process ID [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the pattern programs (i.e., pages 2,3,6,10-13,16,29-35,59) whereas the explicit and implicit use of the term PID (pages 10,13,15,17-19,21,22,27-29,31-34,37-40,44,50-56,59) is taught.].";

And further as per claim 30; this claim is the system of the method claim 4, and is rejected for the same reasons provided for the claim 4 rejection above.

7. As per claim 9; "A method for analyzing a logfile produced by a computer network security system [entire document, as per description in Chapter 5] comprising:

providing a regular expression query associated with a pattern to be searched for in the logfile [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the (i.e., C++) pattern programs).]; and

using the query to search for the pattern in the logfile [entire document, as per description in Chapter 4 (i.e., audit trail)];

wherein the pattern is associated with a *sgid* exploit,

the pattern is associated with processes spawned by a shell, and

using the query to search for the pattern includes

searching for entries showing that the shell has started a process,

storing a process ID of the process, and

searching for entries showing processes with parent process equal to the stored process ID [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the pattern programs (i.e., pages 2,3,6,10-13,16,29-35,59) whereas the explicit and implicit use of the sgid (pages 6,25,30,50-54,60) and PID (pages 10,13,15,17-19,21,22,27-29,31-34,37-40,44,50-56,59) terms is taught.]

wherein the shell comprises a sgid process with effective group ID equal to zero and group ID (gid) not equal to zero.".

### *Response to Amendment*

8. As per applicant's argument concerning the lack of teaching by Crosbie et al of "...wherein the shell comprises a sgid process with effective group ID equal to zero and group ID (gid) not equal to zero ...", the examiner has fully considered the argument and finds it not to

be persuasive. The use of the '... The boolean expressions in IDIOT are expressed in a C-like syntax ... (i.e., see pp 39 et seq.)' aspect such that the boolean expressions are clearly regular expressions per se in the context of search criteria construction. Further, ' ... They are evaluated left-to-right with short circuit evaluation. This means that if a component of the guard causes the whole guard to evaluate to false, evaluation halts. Most guards are specified in conjunctive normal form — a conjunction of clauses. Conjunction is specified using the AND operator, which is && in C (and IDIOT). The guard for the transition exec lpr looks as follows:

```
{
this[ERR] = 0 && PID = this[PID] && PROG = this[PROG] &&
RUID = this[RUID] && (strmatch(".*lpr", this[PROG]) = 1) && this[EUID] = 0;
}
```

This guard is composed of six clauses each separated by a && operator. The full guard is only rue if each of the clauses are individually true. If any clause evaluates to false, the value of the conjunction of these clauses is false, so evaluation halts and the guard evaluates to false... ', clearly encompasses the process initiation and set group/user ID aspects, as broadly interpreted by the examiner, in that via the said "...clauses each separated by a && operator ..." type rules construction, clearly encompasses (at the very least, as far as the parsing and evaluative aspects of the claim limitations) the 'boolean/regular expression' teachings of ' ... a sgid process with effective group ID equal to zero and group ID (gid) not equal to zero.'.

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

## *Conclusion*

10. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum
Patent Examiner

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100